TAMPER SENSING METHOD AND APPARATUS

FIELD OF THE INVENTION

The present invention pertains to security systems and more particularly to the sensing of tampering with respect to devices housed within enclosure members secured together by a connector such as a screw or bolt.

BACKGROUND OF THE INVENTION

The design of data handling devices that may be used for the storage of confidential data will normally require the inclusion of means to detect tampering or the unauthorized disassembly of the device that could be initiated to access the stored confidential data. The smaller the device, the greater the likelihood that it will be lost, mislaid, subject to theft or otherwise be beyond the custody and control of the user and owner of the stored data. In such circumstances, with the device in the possession and control of a party unable to use a password or comply with other requirements to achieve normal access to the stored data, tampering may occur by opening the housing in an attempt to use other extraordinary means to access the data.

In small devices such as a personal digital assistant (PDA) it is important that a non-functional feature incorporated for security purposes not increase the bulk or weight of the device. Ideally the tamper sensing function should be provided, to the extent possible, using structure already incorporated in the device.

In a device which contains confidential data or personal information that would be useful for identity theft, the stored information should be destroyed if the device is disassembled in an attempt to access data which cannot be obtained using the legitimate access to the device.

SUMMARY OF THE INVENTION

The present invention utilizes a central screw which secures the device housing halves

together as a portion of a circuit path that maintains an output node of the circuit at a ground potential. When the screw is removed to separate the housing portions and access the enclosed apparatus to obtain data from the device rather than accessing data through normal device operation using a proper password or complying with other security measures, the output node raises to a voltage level that initiates a response to the tampering. This response may be erasure of the memory or mechanical intervention that makes the device and its stored data useless.

The circuit path through the screw or bolt which secures the enclosure portions is effected by a conductor path applied to the housing surface and a compressive connector that connects the housing surface conductor path to the device ground on the printed circuit board. In many environments the enclosure members have a conductive coating applied to the internal surfaces to suppress electromagnetic interference and this provides the conductive path for the tamper sensing circuit. The tamper sensing circuit can thus be implemented using structure already present in most of the devices in which it would find use.

As shown and described, the screw or bolt which interconnects the two device enclosure portions is electrically connected to the device printed circuit board by passing through an opening in the board and engaging a connector element soldered to the board. This connector element is formed as a flat annular member with flexible or resilient fingers that extend radially inward to engage and provide electrically conductive engagement with a screw which extends therethrough and deflects the fingers. The tamper sensing circuit does not have any material effect on the size or weight of the using device and makes use of several structures existing in the device.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig.1 is a section view of a device incorporating the tamper sensing apparatus and method of the present invention.

Fig. 2 is an enlarged section view of the central portion of Fig. 1.

Fig. 3 is a plan view of the resilient metal annular member used to make electrical contact between the screw connecting the enclosure portions and the device circuitry on the printed

circuit board.

Fig. 4 is a schematic showing of the tamper sensing circuit using the screw connecting the enclosure portions as a part of the circuit.

DETAILED DESCRIPTION

Fig. 1 illustrates an electronic device contained within a housing having an upper enclosure member 12 and a lower enclosure member 14 with respective marginal flanges 15 and 16 which align and position the enclosure members in the assembled condition. A printed circuit board 18 is mounted on the lower enclosure member 14 by screws 20 and 21 which extend through holes in the printed circuit board and are received in axial openings in bosses 24 that are formed as an integral part of the lower enclosure member 14.

Fig. 2 shows an enlarged central portion of the device shown in Fig. 1. The enclosure members 12 and 14 are secured together by a screw 26 which extends through a cylindrical opening 28 in the boss or raised portion 29, formed as an integral portion of the lower enclosure member 14 ,with the terminal end 31 received in a threaded opening 32 in the upper enclosure member 12. The threaded opening in enclosure member 12 is formed in a cylindrical metal insert 33 that is captured in the molded enclosure member boss 35. In the alternative, the threaded opening could be formed in a cylindrical depression in the boss 35. The screw head 37 is received in a recess 39 in the lower enclosure member 14 and screw head 37 is covered by a cap 40, made of the same material as the enclosure member 14, which enables the lower enclosure member to present an uninterrupted lower surface.

The screw 26 also passes through a circular opening 42 in the printed circuit board 18. Electrical contact between the screw 26 and a circuit path 44 on printed circuit board 18 is effected by a resilient metal annular member 46. As seen in Fig. 3, the annular member 44 has a continuous outer annulus 47 and a portion radially inward that includes radially extending cuts or separations 48 to form a series of inwardly extending finger portions 49 that can be deflected. As assembled in Fig. 2, the outer annulus 47 of member 46 is soldered to the printed circuit board 18 enabling electrical connection to printed circuit board conductor path 44. The annular member

fingers 49 terminate in a circular edge 50 having a diameter smaller than that of screw 26, so that when the screw is inserted through the circular member 46 the fingers 49 are deflected to form an electrical contact between annular member 46 and screw 26.

A compressible conductive part 52 is soldered to the printed circuit board and engages the upper enclosure member conductive layer 54 to provide the conductive layer 54 a connection to the card ground circuit 55. The conductive layer 54 is a circuit path extending between the conductive part 52 and the metal insert 33 to cause the screw 26 to be connected to the card ground circuit when installed to engage the threaded insert and secure the upper enclosure member 12 to the lower enclosure member 14.

Although the conductive layer 54 is shown as a circuit path applied to the upper enclosure member inner surface 56, it is frequently unnecessary to make a special provision for this conductor since it is often necessary to apply a metal coating to such enclosure member inner surface 56 to prevent electromagnetic emissions.

Fig. 4 illustrates the tamper sensing circuit effected by the enclosure structure shown in Figs. 1 through 3. The conductive layer 54 is connected through the compressible connector 52 to the card ground 55. The continuous conductive path from the card ground formed by the conductive layer 54, screw 26 (through insert 33), the resilient annular member 46 and printed circuit board circuit path 44; causes node A to be at ground potential. Should the circuit be interrupted by the removal of screw 26, node A would rise to voltage V, indicating the occurrence of tampering and causing the device to respond. Where the security measure is provided to prevent access to confidential data, the device could overwrite the memory or cause hardware damage that would prevent access to stored data.

The length of overlap of the enclosure member marginal flanges 15 and 16 is greater than the length of screw 26 that is received in the enclosure member threaded opening 32. Thus, the screw 26 will disengage from the threaded opening 32 and signal tampering at node A before the enclosure member marginal flanges 15 and 16 cease to overlap. The existence of tampering is thereby signaled prior to access being gained to the interior of the device housing and the device circuitry.

This invention utilizes structure that already exists in the device to perform a large

portion of the function. This minimizes the structure that must be added to support the sensing function. Thus, when tamper sensing is required, it can be provided with little or no impact on the device volume, which is highly restricted in most electronic apparatus environments.

The foregoing description of an embodiment of the invention has been presented for purposes of illustration and description. It is not intended to be exhaustive or limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by the description and illustrations, but rather by the claims appended hereto.